



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/275,722	03/24/1999	DAVID A. LEE	042390.P6526	1130

7590 05/27/2003

WILLIAM W SCHAAL
BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
7TH FLOOR
LOS ANGELES, CA 90025

EXAMINER

LEE, CHI CHUNG

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 05/27/2003

3

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/275,722

Applicant(s)

LEE, DAVID A.

Examiner

Chi-Chung E Lee

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 24 March 1999.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-27 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-27 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 24 March 1999 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892) 4) ☐ Interview Summary (PTO-413) Paper No(s). _____
- 2) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948) 5) ☐ Notice of Informal Patent Application (PTO-152)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 2. 6) ☐ Other:

DETAILED ACTION

1. The IDS (paper # 2) submitted by the applicant has been considered.

Drawings

2. The drawings are objected to because the phrase "KSV2 340" mentioned in page 11 of the specification does not match the title of the reference character "340" in the figure 3. A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.
3. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(4) because reference character "200" has been used to designate both PROCESSOR UNIT and PUKCA in figure 2. A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Art Unit: 2131

Claims 1-18, 19, 23-27 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Notice that the recited steps of claims 1, 11 are purely mathematical operations acting on a given matrix. The claimed invention lacks patentable utility – (notice that the resultant matrix is not utilized for any purpose).

Claims 2-10, 12-18 recite further details of arithmetic operation recited in claims 1, 11 or add additional function elements. Thus they also recite non-statutory subject matter.

Claim 19 is directed to a computer program (i.e. software) comprising several functions (i.e. software). It does not fall within the statutory classes listed in 35 U.S.C. 101.

Claim 23 is directed to a certification authority (i.e. function) comprising a key matrix (i.e. software) in memory and logic (i.e. software) to generate a key selection vector. It does not fall within the statutory classes listed in 35 U.S.C. 101.

Claims 24-27 recite further details of arithmetic operation recited in claim 23. Thus they also recite non-statutory subject matter.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 1-4,11-14,20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lotspiech et al (US 6,118,873 A) in view of Luther (US 5,533,127 A)

Lotspiech is directed to a digital broadcast system provides secure transmission of digital program using a set of device keys

As per claims 1,2, Lotspiech discloses the set of device keys is represent by a two-dimensional matrix including a key dimension (i.e. N rows) and a sets dimension (i.e. M columns), see figure 3 and column 35 lines 20-28. Lotspiech discloses each user device 18 is assigned "N" device keys (i.e. selected secret device keys) from more than two rows of the device key matrix; see column 5 lines 42-54. Lotspiech discloses using an XOR operation on all of the session numbers to render the session key (i.e. a shared secret key), see column 6 lines 29-41. Lotspiech also discloses each session number X_i is encrypted "M" time to render "M" versions of the session number X_i , see column 5 lines 61-65. Lotspiech discloses each user device 18 is assigned "N" devices keys. Lotspiech does not specifically disclose performing the arithmetic operations on matrix keys of at least two selected rows.

Luther's patent (US 5,533,127 A) is directed to a system for encrypting two-dimensional data such as image data by multiple encryption passes through the data. Luther discloses randomly selecting m and n from two-dimension data matrix. Luther discloses with m equal to 3, the third, sixth, ninth, twelfth and each successive third following row though row M are encrypted (i.e. select more than two rows), see column 3 lines 25-37.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to select all row of a specific column to be encrypted by each encryption pass.

One of ordinary skill to the art would have been motivated to encrypt more than two rows based on the arithmetic operation $\text{MOD}(\text{col}, n)$ to determine which rows are encrypted, see column 7 lines 36-55

As per claims 3-4, Luther discloses the single pass m and S are selected (i.e. vector (m, S)) will determine which rows are going to be encrypted, see figure 6

As per claims 11,12, Lotspiech discloses the set of device keys is represent by a two-dimensional matrix including a key dimension (i.e. N rows) and a sets dimension (i.e. M columns), see figure 3 and column 35 lines 20-28. Lotspiech discloses each user device 18 is assigned " N " device keys (i.e. selected secret device keys) from more than two rows of the device key matrix; see column 5 lines 42-54. Lotspiech discloses using an XOR operation on all of the session numbers to render the session key (i.e. a shared secret key), see column 6 lines 29-41. Lotspiech also discloses each session number X_i is encrypted " M " time to render " M " versions of the session number X_i , see column 5 lines 61-65.

Lotspiech discloses each user device 18 is assigned " N " devices keys, Lotspiech does not specifically disclose performing the arithmetic operations on matrix keys of at least two selected columns.

Luther's patent (US 5,533,127 A) is directed to a system for encrypting two-dimensional data such as image data by multiple encryption passes through the data. Luther discloses randomly selecting m and n from two-dimension data matrix. Luther discloses with m equal to

Art Unit: 2131

3, the third, sixth, ninth, twelfth and each successive third following column though N are encrypted (i.e. select more than two columns), see column 4 lines 58-67.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to select all column of a specific row to be encrypted by each encryption pass.

One of ordinary skill to the art would have been motivated to encrypt more than two columns based on the arithmetic operation $\text{MOD}(\text{row}, m)$ to determine which columns are encrypted.

As per claims **13-14**, Luther discloses the single pass n and S are selected (i.e. vector (n, S)) will determine which columns are going to be encrypted, see figure 7 and column 4 lines 43-57.

As per claim **20**, Lotspiech teaches a network 10 substantially comprising a video device 20 (i.e. first digital platform) that can communicate with a digital television 22; a licensing Agency Computer 12 (i.e. certification authority) in communication with the first digital platform. The computer 12 having access to a key matrix (see figure 3) featuring matrix device keys arranged in according with a first dimension (i.e. "i") and a second dimension (i.e. "j") as shown, generating a first key select vector inherit in order to select the highlighted entries providing a first set of secret device keys produced from selected device matrix keys of the key matrix. However, Lotspiech's computer is not expressly disclosed as a certification authority.

It would have been obvious to a person of ordinary skill in the art at the time invention was made to name the computer as certification authority that includes the encryption module to determined that at least one device has been comprised, see column 6 lines 58-65.

Art Unit: 2131

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chi-Chung E Lee whose telephone number is 703-306-4153.

The examiner can normally be reached on 8 am - 5 pm, Mon. - Fri..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gail O Hayes can be reached on 703-305-9711. The fax phone numbers for the organization where this application or proceeding is assigned are 703-746-7239 for regular communications and 703-746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Chi-Chung Lee
May 12, 2003


GAIL HAYES
SUPERVISORY PATENT EXAMINER
BIOLOGY CENTER 2100